REMARKS

These remarks are in response to the Final Office Action dated September 6, 2007 (Office Action). As this reply is timely filed, no fee is believed due. Claims 4, 6, 9, 17, 18, 19, and 20 have been amended. Support for these amendments can be found in paragraphs 3, 19, 21-23, and throughout Applicants' specification. No new matter has been introduced. Claims 1-20 and 22 now are pending.

Within these remarks, Applicants may discuss more than one claim concurrently or more than one element from different claims concurrently. This "grouping" of claims and/or elements of claims is solely to track the grouping of claims and reasoning set forth in the Office Action. Though one or more elements of different claims may refer to similar or the same subject matter, the concurrent treatment of two or more claims and/or features of different claims does not, in and of itself, imply that such claims and/or features do refer to the same subject matter.

Applicants are proceeding with the understanding that the reference to U.S. Patent No. 5,409,661 was a typographical error. Applicants presume that U.S. Patent No. 5,408,661 to Kuranaga (Kuranaga) was the intended citation.

Rejections under 35 U.S.C. § 112

Claims 20 and 22 have been rejected under 35 U.S.C. § 112, first paragraph, for failing to comply with the written description requirement. In particular, the phrases "computer program product" and "computer-usable medium" have been objected to for not being previously disclosed in the specification. The phrase "computer program product" is used within Applicants' specification at paragraph 22, however, Claims 20 and 22 have been amended to more clearly point out the present invention. The phrase "computer-usable medium" has been amended to read "computer-readable medium." Computer-readable media, including memory elements, are disclosed throughout Applicants' specification as being included within a programmable logic device, such as a field programmable gate array (FPGA). Moreover, memory is inherently included within computer systems as described within paragraphs 21-22 of Applicants' specification. For these reasons, withdrawal of the 35 U.S.C. § 112, first paragraph, rejection of claims 20 and 22 is respectfully requested.

Rejections under 35 U.S.C. § 102(b)

Claims 1, 4-12, 14, 20, and 22 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,356,637 to Garnett (Garnett). Applicants respectfully traverse the rejection of claim 1. Claim 1 recites "wherein the configuration data register cannot be read by the microcontroller after the decryptor is used." In support, the Office Action cites FIG. 1; FIG. 6 items 3 and 17; column 5, lines 52-60; and column 7, lines 5-13 and 35-57.

Column 5, lines 52-60 disclose that the functional portion of the FPGA can be formed of volatile elements such as SRAM or other technologies that "fulfill the requirement of compatibility with the technology used for the other FPGA components". This passage of Garnett does not teach or suggest that the configuration data register cannot be read by the microcontroller after the decryptor is used.

At column 7, lines 5-13, Garnett states:

> By contrast to the preceding embodiments, dedicated decryption circuitry is not provided, but rather the decryption function is subsumed in the functional portion 3 of the FPGA and in a state machine 17. The state machine 17 is configured to detect completion of decryption of a set of configuration data and, in response thereto, to generate an output on communication link 25 to the functional portion 3 of the FPGA. The role of the state machine 17 will be more readily understood after the following discussion of the design of the functional portion 3 of the FPGA.

While the state machine can detect when decryption is complete, nothing in the above passages teaches or suggests that the data configuration register cannot be read by the microcontroller after the decryptor is used.

At column 7, lines 35-57, Garnett discloses the operation of configuration logic blocks (CLBs) that are coupled to multiple registers. The main register is used to program the CLB. The holding register is used to store alternate configuration data for the CLB. The main register can receive a reset signal which loads configuration data that configures the CLB to a default state that can decrypt configuration data. The decrypted configuration data can be loaded into the holding register. Upon receiving a signal from the state machine, the contents of the holding register can be loaded into

the main register, thereby causing the CLB to be programmed according to the decrypted configuration data.

This passage also fails to teach or suggest that the configuration data register cannot be read by the microcontroller after the decryptor is used. After the CLB decrypts the encrypted configuration data, the decrypted configuration data is loaded into the holding register. At some point, the decrypted configuration data can be loaded into the primary register to configure the CLB. Garnett does not teach or suggest any mechanism that would prevent reading of the decrypted configuration data from either the main or holding registers. Garnett further does not teach that any configuration information is securely wiped from either the primary register or the holding register.

Assuming arguendo that Garnett does wipe the configuration data, wiping data is not the same as the case where the controller cannot read the configuration data register. More particularly, wiping the data ensures that when the register is read, only garbage data, e.g., zeroes, will be obtained. Still, the holding register and/or the main register would be read. Garnett teaches only that when the CLB is reconfigured, the functionality of the CLB can change. At no point within the discussion cited in column 7 does Garnett teach or suggest that the data register, e.g., primary or holding registers, cannot be read by the microcontroller. In fact, Garnett lacks any discussion as to securing the primary register or the holding register from being read.

Claim 4, as amended, recites "wherein the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware that selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory."

Garnett does not teach or suggest this feature. In referring to claim 2, the Office Action concedes that Garnett does not disclose that "the microcontroller stores key data in the key storage register, but the microcontroller cannot read from the key storage register". Claim 4 is directed to "selectively" enabling access. Garnett does not disclose such a feature.

Though claim 4 has been rejected under 35 U.S.C. § 102(b), Applicants note that neither U.S. Patent No. 6,366,117 to Pang et al. (Pang) nor Kuranaga teaches or suggests this feature. Pang, for example, in column 16, discusses the use of a "ISC_PROGRAM_SECURITY" instruction. Kuranaga relates to virtual memory management and teaches a technique for determining whether an instruction is within RAM according to whether the program counter is within a minimum and maximum virtual address. Neither reference teaches or suggests a feature in which access by the microcontroller to the key storage register is selectively enabled according to the program counter of the microcontroller being within a range of addresses corresponding to the software decryptor within memory. In short, neither Garnett, Pang, Kuranaga, nor any combination thereof teaches or suggests the elements recited in claim 4.

Claim 6, as amended, recites that "the microcontroller further receives a configuration boot program comprising the decryptor in programmatic form along with the encrypted bitstream comprising encrypted configuration data to be loaded into the configuration data register." In the Response to Arguments section, the Office Action states that "[s]ince the on-board memory is used specifically to store keys, it is inherent that the configuration data passed to the FPGA during startup would include boot data. A boot program is necessary in a chip that includes state changes as well as global resets, all of which come from within the chip and not from external sources." The Applicants respectfully disagree and believe this statement reads too much into Garnett.

Garnett does not disclose how the FPGA is initially configured to decrypt data. In fact, Garnett seems to presume that the FPGA is preconfigured to perform such operations. For example, in column 6, Garnett discusses that the decryption logic can decrypt FPGA configuration data using the keys. Garnett does not disclose how the FPGA is initially configured to perform this operation, but rather presumes that the FPGA has been pre-configured to do so. Column 7 discusses an FPGA embodiment in which the default state of the FPGA can decrypt data. Here too Garnett presumes the FPGA effectively is preconfigured to perform decryption.

Garnett simply does not teach or suggest that a boot program specifying the decryptor in programmatic form can be loaded as part of the bitstream that also specifies the encrypted configuration data for the FPGA. Garnett presumes decryption functionality to already exist in the FPGA when the encrypted bitstream is loaded.

Claims 9, 12, and 20 recite one or more features which have been addressed above. As such, these claims are believed to be allowable. The remaining claims rejected under Garnett also are believed to be allowable in view of their own merits and further by virtue of their dependence upon underlying base claim(s) discussed above. As Garnett does not teach or suggest each limitation recited in the Applicants' claims, withdrawal of the 35 U.S.C. § 102(b) rejection of claims 1, 4-12, 14, 20, and 22 is respectfully requested.

Rejections Under 35 U.S.C. § 103(a)

Claims 2, 3, 13, and 15-18 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Garnett in view of Pang. Pang fails to cure the deficiencies of Garnett.

Claim 17, as amended, recites that "the steps of loading the decryptor with data from the key register and loading the decryptor with data from the microcontroller comprises selectively enabling access to the key register by allowing the microcontroller access only when a program counter of the microcontroller specifies an address within an address range of the decryptor." Applicants' remarks relating to claim 4 are pertinent to claim 17.

Claim 18, as amended, recites that "logic circuitry limit[s] access to the key register from the microcontroller data bus using specified addresses of the non-volatile memory corresponding to the decryptor engine and a received program counter value of a microcontroller." Again, neither Pang nor Garnet teaches or suggests such a feature.

The remaining claims rejected under the combination of Garnett and Pang are believed to be allowable in view of their dependency upon underlying base claim(s) and in view of their own merits. Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection of claims 2, 3, 13, and 15-18 is respectfully requested.

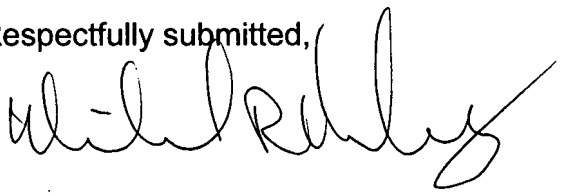
Claim 19 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Garnett and Pang in view of Kuranaga. As noted with respect to claim 4, Kuranaga fails to cure the deficiencies of both Garnett and Pang as Kuranaga teaches a technique for determining whether an instruction must be fetched according to the virtual addresses currently stored in RAM. Neither Garnett, Pang, Kuranaga, nor any combination thereof teaches or suggests that access to a non-volatile memory can be limited using specified addresses of the non-volatile memory corresponding to the decryptor engine and a received program counter value of a microcontroller. Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection of claim 19 is respectfully requested.

CONCLUSION

All claims should be now be in condition for allowance and a Notice of Allowance is respectfully requested.

If there are any questions, the applicants' attorney can be reached at Tel: 408-879-6149.

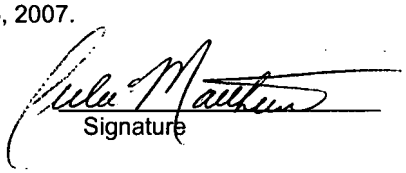
Respectfully submitted,



Michael R. Hardaway
Attorney for Applicants
Reg. No. 52,992

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on November 6, 2007.

Julie Matthews
Name



Signature